2015-11-04

Generalized bent functions and their Gray images

Martinsen, Thor

American Mathematical Society

arXiv:1511.01438v1 [cs.IT] 4 Nov 2015

http://hdl.handle.net/10945/47518

Generalized bent functions and their Gray images

Thor Martinsen[1], Wilfried Meidl[2],
Pantelimon Stănică[1]

[1]Department of Applied Mathematics,
Naval Postgraduate School, Monterey, CA 93943-5212, U.S.A.;
Email: {tmartins,pstanica}@nps.edu
[2]Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria;
Email: meidlwilfried@gmail.com

November 5, 2015

Abstract

In this paper we prove that generalized bent (gbent) functions defined on $\mathbb{Z}_2^n$ with values in $\mathbb{Z}_{2^k}$ are regular, and find connections between the (generalized) Walsh spectrum of these functions and their components. We comprehensively characterize generalized bent and semibent functions with values in $\mathbb{Z}_{16}$, which extends earlier results on gbent functions with values in $\mathbb{Z}_4$ and $\mathbb{Z}_8$. We also show that the Gray images of gbent functions with values in $\mathbb{Z}_{2^k}$ are semibent/plateaued when $k = 3, 4$.

1 Introduction

Let $\mathbb{V}_n$ be an n-dimensional vector space over $\mathbb{F}_2$ and for an integer q, let $\mathbb{Z}_q$ be the ring of integers modulo q. We label the real and imaginary parts of a complex number $z = \alpha + \beta i$, $\alpha, \beta \in \mathbb{R}$, by $\Re(z) = \alpha$ and $\Im(z) = \beta$, respectively. For a *generalized Boolean function* f from $\mathbb{V}_n$ to $\mathbb{Z}_q$ the *generalized Walsh-Hadamard transform* is the complex valued function

$$\mathcal{H}_f^{(q)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{V}_n} \zeta_q^{f(\mathbf{x})}(-1)^{\langle \mathbf{u},\mathbf{x}\rangle}, \quad \zeta_q = e^{\frac{2\pi i}{q}},$$

where $\langle \mathbf{u}, \mathbf{x} \rangle$ denotes a (nondegenerate) inner product on $\mathbb{V}_n$ (we shall use ζ, $\mathcal{H}_f$, instead of ζ_q, respectively, $\mathcal{H}_f^{(q)}$, when q is fixed). In this article we always identify V_n with the vector space $\mathbb{F}_2^n$ of n-tuples over $\mathbb{F}_2$, and we use the regular scalar (inner) product $\langle \mathbf{u}, \mathbf{x} \rangle = \mathbf{u} \cdot \mathbf{x}$. We denote the set of all generalized Boolean functions by $\mathcal{GB}_n^q$ and when $q = 2$, by $\mathcal{B}_n$. A function $f : \mathbb{V}_n \to \mathbb{Z}_q$ is called *generalized bent* (*gbent*) if $|\mathcal{H}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$.

We recall that for $q = 2$, where the generalized Walsh-Hadamard transform of f reduces to the conventional *Walsh-Hadamard transform*

$$\mathcal{W}_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}},$$

a function f for which $|\mathcal{H}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$ is called a *bent* function. Further recall that $f \in \mathcal{B}_n$ is called *plateaued* if $|\mathcal{W}_f(\mathbf{u})| \in \{0, 2^{(n+s)/2}\}$ for all $\mathbf{u} \in \mathbb{V}_n$ for a fixed integer s depending on f (we also call f then *s-plateaued*). If $s = 1$ (n must then be odd), or $s = 2$ (n must then be even), we call f semibent. With this notation a semibent function is an s-plateaued Boolean function with smallest possible $s > 0$. Accordingly we call a function $f \in \mathcal{GB}_n^q$, with $q = 2^k$, $k > 1$ (the case in which we will be most interested), *generalized plateaued* if $|\mathcal{H}_f(\mathbf{u})| \in \{0, 2^{(n+s)/2}\}$ for all $\mathbf{u} \in \mathbb{V}_n$ and some integer s, and *generalized semibent* (*gsemibent*, for short) if $|\mathcal{H}_f(\mathbf{u})| \in \{0, 2^{(n+1)/2}\}$ for all $\mathbf{u} \in \mathbb{V}_n$. Note that differently to a Boolean function, where $k = 1$, a generalized Boolean function $f \in \mathcal{GB}_n^{2^k}$, $k > 1$, can be generalized 1-plateaued also if n is even.

If f is gbent such that for every $\mathbf{u} \in \mathbb{V}_n$, we have $\mathcal{H}_f(\mathbf{u}) = 2^{n/2} \zeta_q^{f^*(\mathbf{u})}$ for some function $f^* \in \mathcal{GB}_n^q$, then we call f a *regular* gbent function. Similar as for bent functions we call f^* the *dual* of f. With the same argument as for the conventional bent functions we can see that the dual f^* is also gbent and $(f^*)^* = f$.

The sum

$$\mathcal{C}_{f,g}(\mathbf{z}) = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{f(\mathbf{x}) - g(\mathbf{x} \oplus \mathbf{z})}$$

is the *crosscorrelation* of f and g at $\mathbf{z}$. The *autocorrelation* of $f \in \mathcal{GB}_n^q$ at $\mathbf{u} \in \mathbb{V}_n$ is $\mathcal{C}_{f,f}(\mathbf{u})$ above, which we denote by $\mathcal{C}_f(\mathbf{u})$. Two functions $f, g \in \mathcal{GB}_n^q$ are said to have *complementary autocorrelation* if and only if $\mathcal{C}_f(\mathbf{u}) + \mathcal{C}_g(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{V}_n \setminus \{0\}$.

Let $f : \mathbb{V}_m \to \mathbb{Z}_q$. If $2^{k-1} < q \leq 2^k$, we associate a unique sequence of Boolean functions $a_i : \mathbb{V}_m \to \mathbb{F}_2$, $1 \leq i \leq k$, such that

$$f(\mathbf{x}) = a_1(\mathbf{x}) + \cdots + 2^{k-1} a_k(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{V}_m.$$

If $q = 2^k$, following Carlet [1], we further define the *generalized Gray map* $\psi(f) : \mathcal{GB}_n^q \to \mathcal{B}_{n+k-1}$ by

$$\psi(f)(\mathbf{x}, y_1, \ldots, y_{k-1}) = \bigoplus_{i=1}^{k-1} a_i(\mathbf{x}) y_i \oplus a_k(\mathbf{x}).$$

It is known [1] that the reverse image of the Hamming distance by the generalized Gray map is a translation-invariant distance.

Generalizations of Boolean bent functions, like negabent functions and the more general class of gbent functions have lately attracted increasing attention, see e.g. [2, 3, 4, 6, 8, 9, 10, 11, 12, 13, 14] and references therein.

In [10, 12] gbent functions $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x})$ in $\mathcal{GB}_n^4$ and $f = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2 a_3(\mathbf{x})$ in $\mathcal{GB}_n^8$ were completely characterized in terms of properties of the Boolean functions $a_i(\mathbf{x})$. In particular, relations between gbentness of f and bentness of associated Boolean functions have been investigated.

In this paper we analyze relations between gbent functions in $\mathcal{GB}_n^{2^k}$ and associated (generalized) Boolean functions. In Section 2, some preliminary results are shown, which we will use in the sequel. In particular we show that every gbent function in $\mathcal{GB}_n^{2^k}$ is regular. In Section 3 we comprehensively characterize gbent functions in $\mathcal{GB}_n^{16}$ in terms of associated Boolean functions, as well as in terms of associated functions in $\mathcal{GB}_n^4$, which extends results of [10, 12] on gbent functions in $\mathcal{GB}_n^4$ and $\mathcal{GB}_n^8$. Furthermore we analyze generalized semibent functions in $\mathcal{GB}_n^{16}$ in terms of associated Boolean functions. We show in Section 4 that the Gray image of a gbent function in $\mathcal{GB}_n^8$, $\mathcal{GB}_n^{16}$ is semibent, respectively, 3-plateaued, which also extends a result in [12]. Finally, in Section 5 we analyze the relations between gbent functions in $\mathcal{GB}_n^{2^k}$ and their components for general $k > 1$.

2 Preliminaries

We start with a theorem about the regularity of gbent functions, which is also of independent interest. We prove the result by modifying a method of Kumar, Scholtz and Welch [5].

Theorem 1. *All gbent functions in $\mathcal{GB}_n^{2^k}$ are regular.*

Proof. If $k = 1$, the result is known, as we are dealing with classical bent functions. Let $k \geq 2$. Let $\zeta = e^{\frac{2\pi i}{2^k}}$ be a 2^k-primitive root of unity. It is known that $\mathbb{Z}[\zeta]$ is the ring of algebraic integers in the cyclotomic field $\mathbb{Q}(\zeta)$.

We recall some facts from [5] (we change the notations slightly). The decomposition for the ideal generated by 2 in $\mathbb{Z}[\zeta]$ has the form $\langle 2\rangle = P^{2^{k-1}}$, where $P = \langle 1-\zeta\rangle$ is a prime ideal in $\mathbb{Z}[\zeta]$. The decomposition group

$$G_2 = \{\sigma \text{ in the Galois group of } \mathbb{Q}(\zeta)/\mathbb{Q} \mid \sigma(P) = P\}$$

contains also the conjugation isomorphism $\sigma^*(z) = z^{-1}$ (Proposition 2 in [5]). Observe that $\mathcal{H}_f^{(2^k)}(\mathbf{u})\overline{\mathcal{H}_f^{(2^k)}(\mathbf{u})} = 2^k$. Now, as in Property 7 of [5], observing that our generalized Walsh transform is simply $S(f, 2^{k-1}\mathbf{u})$ (in the notations of Kumar et al. [5]; $\mathbf{u}$ is a binary vector in our case), then $\mathcal{H}_f^{(2^k)}(\mathbf{u})$ and $\overline{\mathcal{H}_f^{(2^k)}(\mathbf{u})}$ will generate the same ideal in $\mathbb{Z}[\zeta]$ and so, $2^{-k}(\mathcal{H}_f^{(2^k)}(\mathbf{u}))^2$ is a unit, and consequently, $2^{-k/2}\mathcal{H}_f^{(2^k)}(\mathbf{u})$ is an algebraic integer. Therefore, by Proposition 1 of [5] (which, in fact, it is an old result of Kronecker from 1857), $2^{-k/2}\mathcal{H}_f^{(2^k)}(\mathbf{u})$ must be a root of unity. That alone would still not be enough to show regularity since this root of unity may be in a cyclotomic field outside $\mathbb{Q}(\zeta)$, however, that is not the case here, since the Gauss quadratic sum $G(2^k) = \sum_{i=0}^{2^k-1} \zeta^{i^2} = 2^{k/2}(1+i)$ and so, $\sqrt{2} \in \mathbb{Q}(\zeta)$. □

From the definition of a Boolean bent function via the Walsh-Hadamard transform we immediately obtain the following equivalent definition, where we denote the support of a Boolean function f by $\mathrm{supp}(f) := \{\mathbf{x} \in \mathbb{V}_n : f(\mathbf{x}) = 1\}$: A Boolean function $f : \mathbb{V}_n \to \mathbb{F}_2$ is bent if and only if for every $\mathbf{u} \in \mathbb{V}_n$ the function $f_{\mathbf{u}}(\mathbf{x}) := f(\mathbf{x}) \oplus \mathbf{u}\cdot\mathbf{x}$ satisfies $|\mathrm{supp}(f_{\mathbf{u}})| = 2^{n-1} \pm 2^{n/2}$. Our next target is to show an analog description for gbent functions. We use the following lemma.

Lemma 2. *Let $q = 2^k$, $k > 1$, $\zeta = e^{2\pi i/q}$. If $\rho_l \in \mathbb{Q}$, $0 \le l \le q-1$ and $\sum_{l=0}^{q-1} \rho_l \zeta^l = r$ is rational, then $\rho_j = \rho_{2^{k-1}+j}$, for $1 \le j \le 2^{k-1}-1$.*

Proof. Since $\zeta^{2^{k-1}+l} = -\zeta^l$ for $0 \le l \le 2^{k-1}-1$, we can write every element z of the cyclotomic field $\mathbb{Q}(\zeta)$ as

$$z = \sum_{l=0}^{2^{k-1}-1} \lambda_l \zeta^l,\ \lambda_l \in \mathbb{Q}, 0 \le l \le 2^{k-1}-1.$$

As $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(q) = 2^{k-1}$ (φ is Euler's totient function), the set

$\{1, \zeta, \ldots, \zeta^{2^{k-1}-1}\}$ is a basis of $\mathbb{Q}(\zeta)$. Since

$$0 = \sum_{l=0}^{q-1} \rho_l \zeta^l - r = (\rho_0 - \rho_{2^{k-1}} - r) + \sum_{l=1}^{2^{k-1}-1} (\rho_j - \rho_{2^{k-1}+j})\zeta^l.$$

the assertion of the lemma follows. □

Proposition 3. *Let $n = 2m$ be even, and for a function $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ and $\mathbf{u} \in \mathbb{V}_n$, let $f_{\mathbf{u}}(\mathbf{x}) = f(\mathbf{x}) + 2^{k-1}(\mathbf{u}\cdot\mathbf{x})$, and let $b_j^{(\mathbf{u})} = |\mathbf{x} \in \mathbb{V}_n \ : \ f_{\mathbf{u}}(\mathbf{x}) = j\}|$, $0 \le j \le 2^k - 1$. Then f is gbent if and only if for all $\mathbf{u} \in \mathbb{V}_n$ there exists an integer $\rho_{\mathbf{u}}$, $0 \le \rho_{\mathbf{u}} \le 2^{k-1} - 1$ such that*

$$b^{(\mathbf{u})}_{2^{k-1}+\rho_{\mathbf{u}}} = b^{(\mathbf{u})}_{\rho_{\mathbf{u}}} \pm 2^m \text{ and } b^{(\mathbf{u})}_{2^{k-1}+j} = b^{(\mathbf{u})}_j, \text{ for } 0 \le j \le 2^{k-1} - 1, j \ne \rho_{\mathbf{u}}.$$

Proof. First suppose that f is gbent. Then by Theorem 1, f is a regular gbent function. Hence

$$\mathcal{H}_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{V}_n} \zeta^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} = \sum_{\mathbf{x}\in\mathbb{V}_n} \zeta^{f(\mathbf{x})+2^{k-1}(\mathbf{u}\cdot\mathbf{x})} = \mathcal{H}_{f_{\mathbf{u}}}(0) = \sum_{j=0}^{2^k-1} b_j^{(\mathbf{u})}\zeta^j = 2^m\zeta^r$$

for some $0 \le r \le 2^k - 1$. With $\rho_{\mathbf{u}} = r$ if $0 \le r \le 2^{k-1} - 1$, and $\rho_{\mathbf{u}} = r - 2^{k-1}$ otherwise, the claim follows from Lemma 2.

The converse statement is verified in a straightforward manner. □

We will frequently use the following easily verified identity.

Lemma 4. *Let z be a complex number. If $s \in \{0, 1\}$, then*

$$z^s = \frac{1 + (-1)^s}{2} + \frac{1 - (-1)^s}{2} z.$$

Let $f \in \mathcal{GB}_n^{2^k}$ be given as $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + \cdots + 2^{k-1}a_k(\mathbf{x})$, $a_i \in \mathcal{B}_n$, $1 \le i \le k$. With the very general Theorem 2 of [12], one can express the generalized Walsh-Hadamard transform $\mathcal{H}_f(\mathbf{u})$ in terms of the Walsh-Hadamard transforms of Boolean functions obtained as sums of $a_i(\mathbf{x})$, $i \in \{1, \ldots, k\}$. As one may expect, this representation in its generality is not quite explicit. As special cases we represent $\mathcal{H}_f^{(2^k)}(\mathbf{u})$ in terms of the Walsh-Hadamard transforms of the Boolean functions $c_1a_1(\mathbf{x}) \oplus \cdots \oplus c_{k-1}a_{k-1}(\mathbf{x}) \oplus a_k(\mathbf{x})$, $c_i \in \mathbb{F}_2$, for $k = 2, 3, 4$ explicitly in the following lemma. For $k = 2$ and $k = 3$ see also Lemma 3.1 in [10] and Lemma 17 in [12].

Lemma 5. *The following statements are true:*

(*i*) *Let* $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) \in \mathcal{GB}_n^4$ *with* $a_1, a_2 \in \mathcal{B}_n$. *The generalized Walsh-Hadamard transform of* f *is given by*

$$2\mathcal{H}_f^{(4)}(\mathbf{u}) = (\mathcal{W}_{a_2}(\mathbf{u}) + \mathcal{W}_{a_1 \oplus a_2}(\mathbf{u})) + i\,(\mathcal{W}_{a_2}(\mathbf{u}) - \mathcal{W}_{a_1 \oplus a_2}(\mathbf{u}))\,.$$

(*ii*) *Let* $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) = 2^2 a_3(\mathbf{x}) \in \mathcal{GB}_n^8$ *with* $a_1, a_2, a_3 \in \mathcal{B}_n$. *The generalized Walsh-Hadamard transform of* f *is given by*

$$4\mathcal{H}_f^{(8)}(\mathbf{u}) = \alpha_0 \mathcal{W}_{a_3}(\mathbf{u}) + \alpha_1 \mathcal{W}_{a_1 \oplus a_3}(\mathbf{u}) + \alpha_2 \mathcal{W}_{a_2 \oplus a_3}(\mathbf{u}) + \alpha_{12} \mathcal{W}_{a_1 \oplus a_2 \oplus a_3}(\mathbf{u}),$$

where $\alpha_0 = 1 + (1 + \sqrt{2})i$, $\alpha_1 = 1 + (1 - \sqrt{2})i$, $\alpha_2 = 1 + \sqrt{2} - i$, $\alpha_{12} = 1 - \sqrt{2} - i$.

(*iii*) *The generalized Walsh-Hadamard transform of* $f \in \mathcal{GB}_n^{16}$ *with* $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2 a_3(\mathbf{x}) + 2^3 a_4(\mathbf{x})$, $a_i \in \mathcal{B}_n$, $1 \le i \le 4$, *is given by*

$$\begin{aligned} 8\mathcal{H}_f^{(16)}(\mathbf{u}) = {} & \alpha_0 \mathcal{W}_{a_4}(\mathbf{u}) + \alpha_1 \mathcal{W}_{a_1 \oplus a_4}(\mathbf{u}) + \alpha_2 \mathcal{W}_{a_2 \oplus a_4}(\mathbf{u}) \\ & + \alpha_3 \mathcal{W}_{a_3 \oplus a_4}(\mathbf{u}) + \alpha_{12} \mathcal{W}_{a_1 \oplus a_2 \oplus a_4}(\mathbf{u}) + \alpha_{13} \mathcal{W}_{a_1 \oplus a_3 \oplus a_4}(\mathbf{u}) \\ & + \alpha_{23} \mathcal{W}_{a_2 \oplus a_3 \oplus a_4}(\mathbf{u}) + \alpha_{123} \mathcal{W}_{a_1 \oplus a_2 \oplus a_3 \oplus a_4}(\mathbf{u}), \end{aligned}$$

where

$$\begin{aligned} \alpha_0 &= (1+i)(1+\zeta+\zeta^2+\zeta^3) = 1 + i\left(1 + \sqrt{2} + \sqrt{2\left(2+\sqrt{2}\right)}\right), \\ \alpha_1 &= (1+i)(1-\zeta+\zeta^2-\zeta^3) = 1 + i\left(1 + \sqrt{2} - \sqrt{2\left(2+\sqrt{2}\right)}\right), \\ \alpha_2 &= (1+i)(1+\zeta-\zeta^2-\zeta^3) = 1 + \sqrt{2\left(2-\sqrt{2}\right)} + i\left(1-\sqrt{2}\right), \\ \alpha_3 &= (1-i)(1+\zeta+\zeta^2+\zeta^3) = 1 + \sqrt{2} + \sqrt{2\left(2+\sqrt{2}\right)} - i, \\ \alpha_{12} &= (1+i)(1-\zeta-\zeta^2+\zeta^3) = 1 - \sqrt{2\left(2-\sqrt{2}\right)} + i\left(1-\sqrt{2}\right), \\ \alpha_{13} &= (1-i)(1-\zeta+\zeta^2-\zeta^3) = 1 + \sqrt{2} - \sqrt{2\left(2+\sqrt{2}\right)} - i, \\ \alpha_{23} &= (1-i)(1+\zeta-\zeta^2-\zeta^3) = 1 - \sqrt{2} - i\left(1 + \sqrt{2\left(2-\sqrt{2}\right)}\right), \\ \alpha_{123} &= (1-i)(1-\zeta-\zeta^2+\zeta^3) = 1 - \sqrt{2} - i\left(1 - \sqrt{2\left(2-\sqrt{2}\right)}\right). \end{aligned}$$

Proof. One can show all cases by straightforward direct calculations (using Lemma 4) or by applying [12, Theorem 2]. For $k = 4$ both approaches are quite cumbersome. We will only perform the calculations for (i), where $k = 2$.

By Lemma 4, we write

$$\begin{aligned}
2\mathcal{H}_f^{(4)}(\mathbf{u}) &= 2\sum_{\mathbf{x}\in\mathbb{F}_2^n} i^{a_1(\mathbf{x})+2a_2(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \left((1+(-1)^{a_1(\mathbf{x})}) + i(1-(-1)^{a_1(\mathbf{x})})\right)(-1)^{a_2(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= (1+i)\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{a_2(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} + (1-i)\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{a_1(\mathbf{x})\oplus a_2(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= (1+i)\mathcal{W}_{a_2}(\mathbf{u}) + (1-i)\mathcal{W}_{a_1\oplus a_2}(\mathbf{u}) \\
&= (\mathcal{W}_{a_2}(\mathbf{u}) + \mathcal{W}_{a_1\oplus a_2}(\mathbf{u})) + i\left(\mathcal{W}_{a_2}(\mathbf{u}) - \mathcal{W}_{a_1\oplus a_2}(\mathbf{u})\right).
\end{aligned}$$

□

Lemma 6. *The set* $\left\{1, \sqrt{2}, \sqrt{2-\sqrt{2}}, \sqrt{2+\sqrt{2}}\right\}$ *is linear independent over* $\mathbb{Z}$ *(certainly, over* $\mathbb{Q}$*, as well).*

Proof. Assume that there is a nontrivial linear relation of the form

$$a + b\sqrt{2} + c\sqrt{2-\sqrt{2}} + d\sqrt{2+\sqrt{2}} = 0,\ a, b, c, d \in \mathbb{Z}.$$

Without loss of generality, we assume that $\gcd(a, b, c, d) = 1$. By moving the last two terms to the right side and squaring, we obtain

$$a^2 + 2b^2 + 2ab\sqrt{2} = c^2(2-\sqrt{2}) + d^2(2+\sqrt{2}) + 2cd\sqrt{2},$$

that is, $\sqrt{2}(c^2 - d^2 - 2cd + 2ab) = 2c^2 + 2d^2 - a^2 - 2b^2$, and so,

$$\begin{aligned}
c^2 - d^2 - 2cd + 2ab &= 0, \\
2c^2 + 2d^2 - a^2 - 2b^2 &= 0.
\end{aligned}$$

The first equation shows that c, d must have the same parity, and the second shows that $a \equiv 0 \pmod 2$, say $a = 2^r a_1,\ r \geq 1, a_1 \in \mathbb{Z}$. Consequently, $c^2 - d^2 + 2ab \equiv 0 \pmod 4$, which implies that $2cd \equiv 0 \bmod 4$. Therefore $c \equiv d \equiv 0 \bmod 2$, say $c = 2^t c_1, d = 2^u d_1,\ t \geq 1, u \geq 1,\ c_1, d_1 \in \mathbb{Z}$, and by the second equation we have $2^{2t}c_1^2 + 2^{2u}d_1^2 - 2^{2r-1}a_1^2 - b^2 = 0$. From $\gcd(a, b, c, d) = 1$, which implies that b is odd, we see that $2b^2 \equiv 2 \pmod 4$. This yields a contradiction since $2^{2t}c_1^2 \equiv 2^{2u}d_1^2 \equiv 2^{2r}a_1^2 \equiv 0 \pmod 4$. □

Remark 7. *The set* $\{1, \sqrt{2}, \alpha_1 = \sqrt{2-\sqrt{2}}, \alpha_2 = \sqrt{2+\sqrt{2}}\}$ *is actually a basis of* $K = \mathbb{Q}(\sqrt{2}, \alpha_1)$ *over* $\mathbb{Q}$*, the splitting field of* $(x^2-2)(x^4-4x^2+2)$*. Note that* $\alpha_1\alpha_2 = \sqrt{2}$*.*

The following lemma is used several times in the next few sections, and we find it is worth to be noted on its own.

Lemma 8. *Let* $f \in \mathcal{GB}_n^{2^k}$ *with* $f(\mathbf{x}) = g(\mathbf{x}) + 2h(\mathbf{x}), g \in \mathcal{B}_n, h \in \mathcal{GB}_n^{2^{k-1}}$*. Then*

$$2\mathcal{H}_f^{(2^k)}(\mathbf{u}) = (1+\zeta_{2^k})\mathcal{H}_h^{(2^{k-1})}(\mathbf{u}) + (1-\zeta_{2^k})\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u}). \tag{1}$$

Proof. Using Lemma 4, we write

$$\begin{aligned}
2\mathcal{H}_f^{(2^k)}(\mathbf{u}) &= 2\sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta_{2^k}^{g(\mathbf{x})}\zeta_{2^{k-1}}^{h(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \left(1 + (-1)^{g(\mathbf{x})} + (1-(-1)^{g(\mathbf{x})})\zeta_{2^k}\right)\zeta_{2^{k-1}}^{h(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= (1+\zeta_{2^k})\mathcal{H}_h^{(2^{k-1})}(\mathbf{u}) + (1-\zeta_{2^k})\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u}).
\end{aligned}$$

□

3 Complete characterization of generalized bent and semibent functions in $\mathcal{GB}_n^{16}$

In this section we characterize gbent functions in $\mathcal{GB}_n^{16}$ in several ways. We write $f \in \mathcal{GB}_n^{16}$ as

$$\begin{aligned}
f(\mathbf{x}) &= a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2a_3(\mathbf{x}) + 2^3a_4(\mathbf{x}) \\
&= b_1(\mathbf{x}) + 2^2b_2(\mathbf{x}) = a_1(\mathbf{x}) + 2d(\mathbf{x}),
\end{aligned}$$

where $a_i(\mathbf{x}) \in \mathcal{B}_n$, $i = 1,2,3,4$, $b_1(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x})$, $b_2(\mathbf{x}) = a_3(\mathbf{x}) + 2a_4(\mathbf{x})$ are in $\mathcal{GB}_n^4$, and $d(\mathbf{x}) = a_2(\mathbf{x}) + 2a_3(\mathbf{x}) + 2^2a_4(\mathbf{x}) \in \mathcal{GB}_n^8$.

Our objective is to show necessary *and* sufficient conditions on the components $a_1, a_2, a_3, a_4, b_1, b_2, d$ for the gbentness of f. For the conditions on a_1 and d for the gbentness of $a_1(\mathbf{x}) + 2d(\mathbf{x})$ when n is even, we can refer to our general result in Theorem 20 in Section 5. For the special case of gbent functions in $\mathcal{GB}_n^{16}$, n even, it states that $f(\mathbf{x}) = a_1(\mathbf{x}) + 2d(\mathbf{x})$ is gbent if and only if d and $d + 4a_1$ are gbent in $\mathcal{GB}_n^8$ and $\Im\left(\overline{\mathcal{H}_d^{(8)}(\mathbf{u})}\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})\right) = 0$ for all $\mathbf{u} \in \mathbb{V}_n$.

The first target in this section is to show necessary and sufficient conditions on the Boolean functions a_1, a_2, a_3, a_4 for f to be gbent $\mathcal{GB}_n^{16}$ for even as well as for odd n. Secondly, necessary and sufficient conditions on the functions b_1, b_2 for the gbentness of f are given. This complete characterization of gbent functions in $\mathcal{GB}_n^{16}$ extends results in [10, 12] on gbent functions in $\mathcal{GB}_n^4$ and $\mathcal{GB}_n^8$. Finally we also characterize gsemibent functions $f \in \mathcal{GB}_n^{16}$ in terms of a_1, a_2, a_3, a_4.

Theorem 9. *Suppose that* $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2a_3(\mathbf{x}) + 2^3a_4(\mathbf{x})$, $a_i \in \mathcal{B}_n$, $1 \le i \le 4$. *Then* f *is gbent in* $\mathcal{GB}_n^{16}$ *if and only if the conditions* (i) *(if* n *is even), or* (ii) *(if* n *is odd) hold:*

(i) *For all* $c_i \in \mathbb{F}_2$, $i = 1, 2, 3$, *the Boolean function* $c_1a_1 \oplus c_2a_2 \oplus c_3a_3 \oplus a_4$ *is bent, and for all* $\mathbf{u} \in \mathbb{V}_n$ *we have*

$$\begin{aligned}&\mathcal{W}_{a_4}(\mathbf{u})\mathcal{W}_{a_2\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_3\oplus a_4}(\mathbf{u})\mathcal{W}_{a_2\oplus a_3\oplus a_4}(\mathbf{u})\\ &= \mathcal{W}_{a_1\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_3\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2\oplus a_3\oplus a_4}(\mathbf{u}),\ \textit{and}\\ &\mathcal{W}_{a_4}(\mathbf{u})\mathcal{W}_{a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_3\oplus a_4}(\mathbf{u}).\end{aligned}$$

(ii) *For all* $c_i \in \mathbb{F}_2$, $i = 1, 2, 3$, *the Boolean function* $c_1a_1 \oplus c_2a_2 \oplus c_3a_3 \oplus a_4$ *is semibent, and for all* $\mathbf{u} \in \mathbb{V}_n$ *we either have*

$$\begin{aligned}&\mathcal{W}_{a_4}(\mathbf{u})\mathcal{W}_{a_2\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2\oplus a_4}(\mathbf{u}) = \pm 2^{n+1}\ \textit{and}\\ &\mathcal{W}_{a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_2\oplus a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_2\oplus a_3\oplus a_4}(\mathbf{u}) = 0,\end{aligned}$$

or

$$\begin{aligned}&\mathcal{W}_{a_2\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_2\oplus a_4}(\mathbf{u}) = 0\ \textit{and}\\ &\mathcal{W}_{a_3\oplus a_4}(\mathbf{u})\mathcal{W}_{a_2\oplus a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_3\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2\oplus a_3\oplus a_4}(\mathbf{u}) = \pm 2^{n+1}.\end{aligned}$$

Proof. Let $\mathbf{u} \in \mathbb{V}_n$. For $k = 4$, Equation (1) equals

$$2\mathcal{H}_f^{(16)}(\mathbf{u}) = (1 + \zeta_{16})\mathcal{H}_d^{(8)}(\mathbf{u}) + (1 - \zeta_{16})\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u}).$$

Taking norms and squaring, in this case we get

$$\begin{aligned}
4|\mathcal{H}_f^{(16)}(\mathbf{u})|^2 &= \Big((1+\zeta_{16})\mathcal{H}_d^{(8)}(\mathbf{u}) + (1-\zeta_{16})\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})\Big) \\
&\quad \times \Big((1+\overline{\zeta_{16}})\overline{\mathcal{H}_d^{(8)}(\mathbf{u})} + (1-\overline{\zeta_{16}})\overline{\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})}\Big) \\
&= (1+\zeta_{16})(1+\overline{\zeta_{16}})|\mathcal{H}_d^{(8)}(\mathbf{u})|^2 + (1-\zeta_{16})(1-\overline{\zeta_{16}})||\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})|^2 \\
&\quad + (1+\zeta_{16})(1-\overline{\zeta_{16}})\mathcal{H}_d^{(8)}(\mathbf{u})\overline{\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})} \\
&\quad + (1-\zeta_{16})(1+\overline{\zeta_{16}})\bar{\mathcal{H}}_d^{(8)}(\mathbf{u})\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u}) \\
&= (2+\sqrt{2+\sqrt{2}})|\mathcal{H}_d^{(8)}(\mathbf{u})|^2 + (2-\sqrt{2+\sqrt{2}})|\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})|^2 \\
&\quad + 2\sqrt{2-\sqrt{2}}\,\Im\left(\overline{\mathcal{H}_d^{(8)}(\mathbf{u})}\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})\right).
\end{aligned}$$

Equivalently,

$$\begin{aligned}
16\sqrt{2}|\mathcal{H}_f^{(16)}(\mathbf{u})|^2 &= (2+\sqrt{2+\sqrt{2}})4\sqrt{2}|\mathcal{H}_d^{(8)}(\mathbf{u})|^2 + (2-\sqrt{2+\sqrt{2}})4\sqrt{2}|\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})|^2 \\
&\quad + 8\sqrt{4-2\sqrt{2}}\,\Im\left(\overline{\mathcal{H}_d^{(8)}(\mathbf{u})}\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})\right). \qquad (2)
\end{aligned}$$

We denote by A, C, D, W the Walsh-Hadamard transforms $\mathcal{W}_{a_4}(\mathbf{u})$, $\mathcal{W}_{a_2\oplus a_4}(\mathbf{u})$, $\mathcal{W}_{a_3\oplus a_4}(\mathbf{u})$, $\mathcal{W}_{a_2\oplus a_3\oplus a_4}(\mathbf{u})$ (in that order). We denote by B, X, Y, Z the Walsh-Hadamard transforms $\mathcal{W}_{a_1\oplus a_4}(\mathbf{u})$, $\mathcal{W}_{a_1\oplus a_2\oplus a_4}(\mathbf{u})$, $\mathcal{W}_{a_1\oplus a_3\oplus a_4}(\mathbf{u})$, $\mathcal{W}_{a_1\oplus a_2\oplus a_3\oplus a_4}(\mathbf{u})$ (in that order). By Lemma 5(ii), we know that the generalized Walsh-Hadamard transform of any function in $\mathcal{GB}_n^8$, say d and $d+4a_1$ with $d = a_2 + 2a_3 + 2^2a_4$, is of the form

$$\begin{aligned}
4\mathcal{H}_d^{(8)}(\mathbf{u}) &= \alpha_0 A + \alpha_1 C + \alpha_2 D + \alpha_3 W, \\
4\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u}) &= \alpha_0 B + \alpha_1 X + \alpha_2 Y + \alpha_3 Z,
\end{aligned}$$

where $\alpha_0 = 1 + (1+\sqrt{2})i$, $\alpha_1 = 1 + (1-\sqrt{2})i$, $\alpha_2 = 1 + \sqrt{2} - i$, $\alpha_3 = 1 - \sqrt{2} - i$, and moreover that (see also [12, Corollary 18]),

$$4\sqrt{2}|\mathcal{H}_d^{(8)}(\mathbf{u})|^2 = A^2 - C^2 + 2CD + D^2 - 2AW - W^2 + \sqrt{2}(A^2 + C^2 + D^2 + W^2) \qquad (3)$$

$$4\sqrt{2}|\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})|^2 = B^2 - X^2 + 2XY + Y^2 - 2BZ - Z^2 + \sqrt{2}(B^2 + X^2 + Y^2 + Z^2).$$

Furthermore, with straightforward computations we get

$$\begin{aligned}
&8\sqrt{4-2\sqrt{2}}\,\Im\left(\overline{\mathcal{H}_b^{(8)}(\mathbf{u})}\mathcal{H}_{b+4a_1}^{(8)}(\mathbf{u})\right)\\
&=2\sqrt{2-\sqrt{2}}\left(\sqrt{2}\,(BD+WX-AY-CZ)\right.\\
&\quad\left.+BC+BD-AX-WX-AY+WY+CZ-DZ\right)\\
&=2\sqrt{2-\sqrt{2}}\,(BC+BD-AX-WX-AY+WY+CZ-DZ)\\
&\quad+2\sqrt{4-2\sqrt{2}}\,(BD+WX-AY-CZ)
\end{aligned}\tag{4}$$

With (3) and (4) for Equation (2) we obtain

$$\begin{aligned}
&16\sqrt{2}|\mathcal{H}_f^{(16)}(\mathbf{u})|^2\\
&=2(A^2+B^2-C^2+2CD+D^2-2AW-W^2-X^2+2XY+Y^2-2BZ-Z^2)\\
&\quad+2\sqrt{2}(A^2+B^2+C^2+D^2+W^2+X^2+Y^2+Z^2)\\
&\quad+\sqrt{2-\sqrt{2}}\,(A^2-B^2+2BC+C^2+D^2+W^2-2AX-4WX-X^2\\
&\qquad+2WY-Y^2+4CZ-2DZ-Z^2)\\
&\quad+2\sqrt{2+\sqrt{2}}\,(A^2-B^2+BD+CD+D^2-AW+WX-AY-XY\\
&\qquad-Y^2+BZ-CZ).
\end{aligned}\tag{5}$$

Now suppose that f is gbent in $\mathcal{GB}_n^{16}$, i.e., $|\mathcal{H}_f^{(16)}(\mathbf{u})|^2=2^n$. By Lemma 6, $1,\sqrt{2},\sqrt{2-\sqrt{2}},\sqrt{2+\sqrt{2}}$ are $\mathbb{Z}$-linearly independent, and hence we arrive at the following a system of equations (in the variables A,B,C,D,X,Y,Z,W) with solutions in $\mathbb{Z}$:

$$\begin{aligned}
&A^2+B^2+C^2+D^2+W^2+X^2+Y^2+Z^2=2^{n+3}\\
&A^2+B^2-C^2+2CD+D^2-2AW-W^2-X^2+2XY\\
&\qquad\qquad+Y^2-2BZ-Z^2=0\\
&A^2-B^2+2BC+C^2+D^2+W^2-2AX-4WX-X^2\\
&\qquad\qquad+2WY-Y^2+4CZ-2DZ-Z^2=0\\
&A^2-B^2+BD+CD+D^2-AW+WX-AY-XY\\
&\qquad\qquad-Y^2+BZ-CZ=0.
\end{aligned}\tag{6}$$

Let 2^t be the largest power of 2 which divides all, A,B,C,D,X,Y,Z and W, i.e., $A=2^tA_1$, etc., with at least one of the $A_1,B_1,\ldots$ being odd. First, if n is even and $t>\frac{n}{2}$, then $t=\frac{n}{2}+1$ only. Dividing by 2^{2t}, the first equation of (6) becomes $A_1^2+B_1^2+C_1^2+D_1^2+W_1^2+X_1^2+Y_1^2+Z_1^2=2$, which gives the solution $(\pm1,\pm1,0,0,0,0,0,0)$ (and permutations of these

values). However, a simple computation reveals that none of these possibilities also satisfies the last three equations of (6). If n is odd and $t > \frac{n+1}{2}$, then t must be $t = \frac{n+3}{2}$, but this implies that only one value out of $A, B, \ldots$ is nonzero and again, that is impossible to satisfy the last three equations of (6). Assume now that $t < \frac{n}{2}$. The first equation of (6) becomes $A_1^2+B_1^2+C_1^2+D_1^2+W_1^2+X_1^2+Y_1^2+Z_1^2 = 2^{n+3-2t}$, which is divisible by 2^5 (when n is even, since $t \leq \frac{n-2}{2}$), respectively 2^4 (when n is odd, since $t \leq \frac{n-1}{2}$). If n is even, this can only happen if $A_1, B_1, \ldots,$ are all even, that is, $\equiv 0, 2, 4, 6 \pmod 8$, but that contradicts our assumption that t is the largest power of 2 dividing $A, B, \ldots$. If n is odd and $t \leq \frac{n-3}{2}$, the previous argument would work, and if $t = \frac{n-1}{2}$, then $A_1^2 + B_1^2 + C_1^2 + D_1^2 + W_1^2 + X_1^2 + Y_1^2 + Z_1^2 = 16$. One can certainly argue exhaustively, or by considering every residues for $A_1, B_1, \ldots,$ modulo 4 and imposing the condition that the 2nd, 3rd, 4th equations of our system also must be 0 modulo 16, we only get possibilities $(0,0,2,2,0,0,2,2)$, $(0,2,0,2,0,2,0,2)$, $(0,2,2,0,0,2,2,0)$, $(2,0,0,2,2,0,0,2)$, $(2,0,2,0,2,0,2,0)$, $(2,2,0,0,2,2,0,0)$ for $(A_1, B_1, \ldots)$ modulo 4, but that implies that all $A_1, B_1, \ldots$ are even, but that contradicts our assumption that t is the largest power of 2 dividing $\gcd(A, B, \ldots,)$. This shows that the only possibility is $2^t = 2^{n/2}$ if n is even, and $2^t = 2^{(n+1)/2}$ if n is odd.

Thus, one needs to find integer solutions for the equation $A_1^2 + B_1^2 + C_1^2 + D_1^2 + \mathcal{W}_1^2 + X_1^2 + Y_1^2 + Z_1^2 = 8$, for n even, or $A_1^2 + B_1^2 + C_1^2 + D_1^2 + \mathcal{W}_1^2 + X_1^2 + Y_1^2 + Z_1^2 = 4$ for n odd, which also satisfy the last three equations in (6). Again, Mathematica renders the following: if n is even, then $2^{-\frac{n}{2}}(A, C, D, W, B, X, Y, Z)$ (note the order) is one of

$$\begin{array}{ll}
(-1,-1,-1,-1,-1,-1,-1,-1), & (-1,-1,1,1,-1,-1,1,1), \\
(-1,1,-1,1,-1,1,-1,1), & (-1,1,1,-1,-1,1,1,-1), \\
(-1,-1,-1,-1,1,1,1,1), & (-1,-1,1,1,1,1,-1,-1), \\
(-1,1,-1,1,1,-1,1,-1), & (-1,1,1,-1,1,-1,-1,1), \\
(1,-1,-1,1,-1,1,1,-1), & (1,-1,1,-1,-1,1,-1,1), \\
(1,1,-1,-1,-1,-1,1,1), & (1,1,1,1,-1,-1,-1,-1), \\
(1,-1,-1,1,1,-1,-1,1), & (1,-1,1,-1,1,-1,1,-1), \\
(1,1,-1,-1,1,1,-1,-1), & (1,1,1,1,1,1,1,1)
\end{array} \tag{7}$$

and, if n is odd, then $2^{-\frac{n+1}{2}}(A, C, D, W, B, X, Y, Z)$ is one of

$$\begin{array}{ll}
(-1,-1,0,0,-1,-1,0,0), & (-1,1,0,0,-1,1,0,0), \\
(-1,-1,0,0,1,1,0,0), & (-1,1,0,0,1,-1,0,0),
\end{array}$$

$$(0,0,-1,-1,0,0,-1,-1), \qquad (0,0,-1,1,0,0,-1,1),$$
$$(0,0,-1,-1,0,0,1,1), \qquad (0,0,-1,1,0,0,1,-1),$$
$$(0,0,1,-1,0,0,-1,1), \qquad (0,0,1,1,0,0,-1,-1),$$
$$(0,0,1,-1,0,0,1,-1), \qquad (0,0,1,1,0,0,1,1),$$
$$(1,-1,0,0,-1,1,0,0), \qquad (1,1,0,0,-1,-1,0,0),$$
$$(1,-1,0,0,1,-1,0,0), \qquad (1,1,0,0,1,1,0,0).$$

Therefore, in the case of even n we see that if f is gbent, then $a_4, a_2 \oplus a_4, a_3 \oplus a_4, a_2 \oplus a_3 \oplus a_4, a_1 \oplus a_4, a_1 \oplus a_2 \oplus a_4, a_1 \oplus a_3 \oplus a_4, a_1 \oplus a_2 \oplus a_3 \oplus a_4$ are all bent in $\mathcal{B}_n$, such that $\mathcal{W}_{a_4}(\mathbf{u})\mathcal{W}_{a_2\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_3\oplus a_4}(\mathbf{u})\mathcal{W}_{w_2\oplus a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_3\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2\oplus a_3\oplus a_4}(\mathbf{u})$ and $\mathcal{W}_{a_4}(\mathbf{u})\mathcal{W}_{a_3+a_4}(\mathbf{u}) = \mathcal{W}_{a_1+a_4}(\mathbf{u})\mathcal{W}_{a_1+a_3+a_4}(\mathbf{u})$ for every $\mathbf{u} \in \mathbb{V}_n$. It is a straightforward computation to see that under these conditions, f is also gbent in $\mathcal{GB}_n^{16}$.

In the case of odd n we see that if f is gbent, then $a_4, a_2 \oplus a_4, a_3 \oplus a_4, a_2 \oplus a_3 \oplus a_4, a_1 \oplus a_4, a_1 \oplus a_2 \oplus a_4, a_1 \oplus a_3 \oplus a_4, a_1 \oplus a_2 \oplus a_3 \oplus a_4$ are semibent with the extra conditions that $\mathcal{W}_{a_4}(\mathbf{u})\mathcal{W}_{a_2\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2\oplus a_4}(\mathbf{u}) = \pm 2^{n+1}$, and $\mathcal{W}_{a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_2\oplus a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_2\oplus a_3\oplus a_4}(\mathbf{u}) = 0$, or $\mathcal{W}_{a_2\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_2\oplus a_4}(\mathbf{u}) = 0$, and $\mathcal{W}_{a_3\oplus a_4}(\mathbf{u})$ $\mathcal{W}_{a_2\oplus a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_3\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2\oplus a_3\oplus a_4}(\mathbf{u}) = \pm 2^{n+1}$, for all $\mathbf{u} \in \mathbb{F}_2^n$. Reciprocally, it is straightforward to check that under these conditions, f is also gbent in $\mathcal{GB}_n^{16}$. □

Remark 10. *It is not sufficient to only use what is known (see* [7] *for a proof) about the number of solutions for the first equation of* (6)*, that is,* $r_8(2^{n+3}) = \frac{16(8^{n+4}-15)}{7}$ *(of course, counting signs and permutations), since the form of these solutions is not known in general.*

Remark 11. *If in* $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2a_3(\mathbf{x}) + 2^3a_4(\mathbf{x})$ *some of the Boolean functions* a_i*,* $i = 1, 2, 3, 4$*, are the zero function, and hence the value set of* f *is restricted accordingly, then the conditions in Theorem* 9 *of course will simplify. For instance we can immediately infer from Theorem* 9 *that* $f(\mathbf{x}) = a_1(\mathbf{x}) + 2^3a_4(\mathbf{x}) \in \mathcal{GB}_n^{16}$ *is gbent for even* n *if and only if* $a_4, a_1 \oplus a_4$ *are both bent, and never gbent for odd* n*. If* $a_3 = 0$*, i.e.,* f *takes on only values in* $\{0, 1, \ldots, 7\}$*, then* f *is not gbent (which is also quite apparent with a direct argument via the generalized Walsh-Hadamard transform - and similarly holds for functions in* $\mathcal{GB}_n^{2^k}$*).*

We next present the connection between gbentness in $\mathcal{GB}_n^4$ and in $\mathcal{GB}_n^{16}$.

Theorem 12. *Let* $f \in \mathcal{GB}_n^{16}$ *with*

$$f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2a_3(\mathbf{x}) + 2^3a_4(\mathbf{x}) = b_1(\mathbf{x}) + 2^2b_2(\mathbf{x}),$$

where $b_1 = a_1 + 2a_2, b_2 = a_3 + 2a_4 \in \mathcal{GB}_n^4$. *The function* f *is gbent in* $\mathcal{GB}_n^{16}$ *if and only if* $b_2, b_1+b_2, 2b_1+b_2, 3b_1+b_2$ *are gbent in* $\mathcal{GB}_n^4$ *with their generalized Walsh-Hadamard transforms satisfying the following conditions,* (*i*) *for* n *even, respectively,* (*ii*) *for* n *odd, for all* $\mathbf{u} \in \mathbb{V}_n$*:*

(*i*) $2^{-n/2}(\mathcal{H}_{3b_1+b_2}(\mathbf{u}), \mathcal{H}_{b_1+b_2}(\mathbf{u}), \mathcal{H}_{2b_1+b_2}(\mathbf{u}), \mathcal{H}_{b_2}(\mathbf{u}))$ *belongs to one of* $(\epsilon,\epsilon,\epsilon,\epsilon)$, $(\epsilon,\epsilon,-\epsilon,-\epsilon)$, $(\epsilon,-\epsilon,\epsilon i,-\epsilon i)$, $(\epsilon-\epsilon,-\epsilon i,\epsilon i)$, $(\epsilon i,\epsilon i,\epsilon i,\epsilon i)$, $(\epsilon i,\epsilon i,-\epsilon i,-\epsilon i)$, $(\epsilon i,-\epsilon i,\epsilon,-\epsilon)$, $(-\epsilon i,\epsilon i,-\epsilon,\epsilon)$, *where* $\epsilon \in \{\pm 1\}$.

(*ii*) $2^{-(n-1)/2}(\mathcal{H}_{3b_1+b_2}(\mathbf{u}), \mathcal{H}_{b_1+b_2}(\mathbf{u}), \mathcal{H}_{2b_1+b_2}(\mathbf{u}), \mathcal{H}_{b_2}(\mathbf{u}))$ *belongs to one of* $(\epsilon+\mu i,\epsilon+\mu i,\epsilon+\mu i,\epsilon+\mu i)$, $(\epsilon+\mu i,\epsilon+\mu i,-\epsilon-\mu i,-\epsilon-\mu i)$, $(\epsilon+\mu i,-\epsilon-\mu i,\epsilon-\mu i,-\epsilon+\mu i)$, $(\epsilon+\mu i,-\epsilon-\mu i,-\epsilon+\mu i,\epsilon-\mu i)$, *for* $\epsilon,\mu \in \{\pm 1\}$.

Proof. By Lemma 4, the generalized Walsh-Hadamard transform of f (labeling $\zeta := \zeta_{16}$) can be written as

$$\begin{aligned}
\mathcal{H}_f^{(16)}(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta^{b_1(\mathbf{x})+2^2 b_2(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta^{b_1(\mathbf{x})} i^{b_2(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= \frac{1}{4}\sum_{\mathbf{x}\in\mathbb{F}_2^n} \Big(i^{b_1(\mathbf{x})+1}\left(-(-1)^{b_1(\mathbf{x})}\zeta^3 + (-1)^{b_1(\mathbf{x})}\zeta + \zeta^3 - \zeta\right) \\
&+ \left(\zeta^2+1\right)\left(\left(1-(-1)^{b_1(\mathbf{x})}\right)\zeta + 1 + (-1)^{b_1(\mathbf{x})}\right) + \\
&i^{b_1(\mathbf{x})}\left(-(-1)^{b_1(\mathbf{x})}\zeta^2 + (-1)^{b_1(\mathbf{x})} - \zeta^2 + 1\right)\Big) i^{b_2(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= \alpha \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{b_1(\mathbf{x})} i^{b_1(\mathbf{x})} i^{b_2(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} + \beta \sum_{\mathbf{x}\in\mathbb{F}_2^n} i^{b_1(\mathbf{x})} i^{b_2(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&\quad + \gamma \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{b_1(\mathbf{x})} i^{b_2(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} + \delta \sum_{\mathbf{x}\in\mathbb{F}_2^n} i^{b_2(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= \alpha\mathcal{H}_{3b_1+b_2}^{(4)}(\mathbf{u}) + \beta\mathcal{H}_{b_1+b_2}^{(4)}(\mathbf{u}) + \gamma\mathcal{H}_{2b_1+b_2}^{(4)}(\mathbf{u}) + \delta\mathcal{H}_{b_2}^{(4)}(\mathbf{u}),
\end{aligned}$$

where

$$\begin{aligned}
8\alpha &= 2(1+i\zeta-\zeta^2-i\zeta^3) = \left(2-\sqrt{2}+\sqrt{4-2\sqrt{2}}\right) - i\left(\sqrt{2}-\sqrt{4-2\sqrt{2}}\right) \\
8\beta &= 2(1-i\zeta-\zeta^2+i\zeta^3) = \left(2-\sqrt{2}-\sqrt{4-2\sqrt{2}}\right) - i\left(\sqrt{2}+\sqrt{4-2\sqrt{2}}\right) \\
8\gamma &= 2(1-\zeta+\zeta^2-\zeta^3) = \left(2+\sqrt{2}-\sqrt{4+\sqrt{2}}\right) + i\left(\sqrt{2}-\sqrt{4+2\sqrt{2}}\right) \\
8\delta &= 2(1+\zeta+\zeta^2+\zeta^3) = \left(2+\sqrt{2}+\sqrt{4+2\sqrt{2}}\right) + i\left(\sqrt{2}+\sqrt{4+2\sqrt{2}}\right).
\end{aligned} \tag{8}$$

First we assume that $b_2, b_1+b_2, 2b_1+b_2, 3b_1+b_2$ are gbent in $\mathcal{GB}_n^4$, with their generalized Walsh-Hadamard transforms satisfying (i) if n is even respectively (ii) if n is odd. With Equation (8) we get the claim (to ease with the computation, we used a Mathematica program).

Conversely, we assume that f is gbent in $\mathcal{GB}_n^{16}$. With the same notations for the Walsh-Hadamard transforms, A, B, C, D, W, X, Y, Z as in the proof of Theorem 9, by Lemma 5, we have

$$\begin{aligned}
2\mathcal{H}^{(4)}_{3b_1+b_2}(\mathbf{u}) &= (X+W)+i(X-W)\\
2\mathcal{H}^{(4)}_{b_1+b_2}(\mathbf{u}) &= (C+Z)+i(C-Z)\\
2\mathcal{H}^{(4)}_{2b_1+b_2}(\mathbf{u}) &= (B+Y)+i(B-Y)\\
2\mathcal{H}^{(4)}_{b_2}(\mathbf{u}) &= (A+D)+i(A-D).
\end{aligned}$$

From Theorem 9, we already know that $A, B, C, \ldots$ are two or three valued (depending upon the parity of n). Running a short script through the possible values described in Theorem 9, we see that the last claim of our current theorem is true as well. □

With the same approach as in Theorem 9 we can also obtain results on the semibentness of functions in $\mathcal{GB}_n^{16}$.

Theorem 13. *Let $f \in \mathcal{GB}_n^{16}$ be given as $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2a_3(\mathbf{x}) + 2^3a_4(\mathbf{x})$, $a_i \in \mathcal{B}_n$, $1 \le i \le 4$. Then f is gsemibent when n is odd, and generalized 2-plateaued when n is even, if and only if the Boolean function $c_1a_1 \oplus c_2a_2 \oplus c_3a_3 \oplus a_4$ is semibent for all $c_i \in \mathbb{F}_2$, $i = 1, 2, 3$, such that for all $\mathbf{u} \in \mathbb{V}_n$ their Walsh-Hadamard transforms are either all zero, or they satisfy*

$$\begin{aligned}
&\mathcal{W}_{a_4}(\mathbf{u})\mathcal{W}_{a_2+a_4}(\mathbf{u}) = \mathcal{W}_{a_3+a_4}(\mathbf{u})\mathcal{W}_{a_2+a_3+a_4}(\mathbf{u})\\
&= \mathcal{W}_{a_1+a_4}(\mathbf{u})\mathcal{W}_{a_1+a_2+a_4}(\mathbf{u}) = \mathcal{W}_{a_1+a_3+a_4}(\mathbf{u})\mathcal{W}_{a_1+a_2+a_3+a_4}(\mathbf{u}), \text{ and}\\
&\mathcal{W}_{a_4}(\mathbf{u})\mathcal{W}_{a_3+a_4}(\mathbf{u}) = \mathcal{W}_{a_1+a_4}(\mathbf{u})\mathcal{W}_{a_1+a_3+a_4}(\mathbf{u}).
\end{aligned}$$

Proof. Assume that f is gsemibent in $\mathcal{GB}_n^{16}$ when n is odd, respectively generalized 2-plateaued when n is even. Then $|\mathcal{H}_f^{(16)}(\mathbf{u})| \in \{0, \pm 2^{(n+1)/2}\}$ for n odd, respectively, $|\mathcal{H}_f^{(16)}(\mathbf{u})| \in \{0, \pm 2^{(n+2)/2}\}$ for n even. Using the notations of Theorem 9, from Equation (5), we immediately get $A = B = C = D = X = Y = W = Z = 0$ if $\mathcal{H}_f^{(16)}(\mathbf{u}) = 0$. If $|\mathcal{H}_f^{(16)}(\mathbf{u})| = 2^{(n+1)/2}$ (for n odd), respectively, $|\mathcal{H}_f^{(16)}(\mathbf{u})| = 2^{(n+2)/2}$ (for n even), then (5) again yields the system of equations (6) with the one difference that in the first equation the power of 2 on the right side is 2^{n+4}, respectively, 2^{n+5}. With

the same argument as in the proof of Theorem 9 we see that for such $\mathbf{u}$, $2^{-\frac{n+1}{2}}(A, C, D, W, B, X, Y, Z)$ (for n odd), respectively, $2^{-\frac{n+2}{2}}(A, C, D, W, B, X, Y, Z)$ (for n even) can only take the values from Equation (7).
Straightforward one confirms that the converse is also true, and the theorem is shown. □

Remark 14. *Again, if some to the Boolean functions a_i, $i = 1, 2, 3, 4$, are the zero function, then the conditions in Theorem 13 further simplify. For instance, we can immediately see that $f(\mathbf{x}) = a_1(\mathbf{x}) + 2^3 a_4(\mathbf{x}) \in \mathcal{GB}_n^{16}$ is gsemibent if n is odd, respectively, generalized 2-plateaued if n is even, if and only $a_4, a_1 \oplus a_4$ are both semibent with $|\mathcal{W}_{a_4}(\mathbf{u})| = |\mathcal{W}_{a_1 \oplus a_4}(\mathbf{u})|$, for all $\mathbf{u} \in \mathbb{F}_2^n$.*

4 Gbents in $\mathcal{GB}_n^8, \mathcal{GB}_n^{16}$ and their Gray image

It was shown in [12] that $f \in \mathcal{GB}_n^4$, with $f(\mathbf{x}) = a_1 + 2a_2(\mathbf{x})$, $a_1, a_2 \in \mathcal{B}_n$, is gbent if and only if the Gray image $\psi(f)$ is bent if n is odd, or semibent and the associated a_2 and $a_1 \oplus a_2$ have complementary autocorrelation if n is even. It is the purpose of this section to extend this result. We show that the Gray image of every gbent function in $\mathcal{GB}_n^8$ is semibent, and the Gray image of every gbent function in $\mathcal{GB}_n^{16}$ is semibent if n is odd, and 3-plateaued if n is even. We start with a lemma.

Lemma 15. *Let $n, k \geq 2$ be positive integers and $F : \mathbb{V}_{n+k-1} \to \mathbb{F}_2$ be defined by $F(\mathbf{x}, y_1, y_2, \ldots, y_{k-1}) = a_k(\mathbf{x}) \oplus \bigoplus_{i=1}^{k-1} y_i a_i(\mathbf{x})$, where $a_i \in \mathcal{B}_n$, $1 \leq i \leq k$. Denote by $\mathbf{a}(\mathbf{x})$ the vectorial Boolean function $\mathbf{a}(\mathbf{x}) = (a_1(\mathbf{x}), \ldots, a_{k-1}(\mathbf{x}))$ and let $\mathbf{u} \in \mathbb{V}_n$ and $\mathbf{v} = (v_1, \ldots, v_{k-1}) \in \mathbb{V}_{k-1}$. The Walsh-Hadamard transform of F at $(\mathbf{u}, \mathbf{v})$ is then*

$$\mathcal{W}_F(\mathbf{u}, v_1, \ldots, v_{k-1}) = \sum_{\alpha \in \mathbb{V}_{k-1}} (-1)^{\alpha \cdot \mathbf{v}} \mathcal{W}_{a_k \oplus \alpha \cdot \mathbf{a}}(\mathbf{u}).$$

Proof. We will show our claim by induction on k. For $k = 2$ we have

$$\begin{aligned}
\mathcal{W}_F(\mathbf{u}, v_1) &= \sum_{\substack{\mathbf{x} \in \mathbb{V}_n \\ y_1 \in \mathbb{F}_2}} (-1)^{y_1 a_1(\mathbf{x}) \oplus a_2(\mathbf{x})} (-1)^{v_1 y_1 \oplus \mathbf{u} \cdot \mathbf{x}} \\
&= \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{a_2(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}} + \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{a_1(\mathbf{x}) \oplus a_2(\mathbf{x})} (-1)^{v_1 \oplus \mathbf{u} \cdot \mathbf{x}} \\
&= \mathcal{W}_{a_2}(\mathbf{u}) + (-1)^{v_1} \mathcal{W}_{a_1 \oplus a_2}(\mathbf{u}).
\end{aligned}$$

Now let

$$F(\mathbf{x}, y_1, \ldots, y_k) = F_1(\mathbf{x}, y_1, \ldots, y_{k-1}) \oplus y_k a_k(\mathbf{x}), \text{ where}$$
$$F_1(\mathbf{x}, y_1, \ldots, y_{k-1}) = a_{k+1}(\mathbf{x}) \oplus \bigoplus_{i=1}^{k-1} y_i a_i(\mathbf{x}).$$

Then

$$\mathcal{W}_F(\mathbf{u}, \mathbf{v}, v_k) = \mathcal{W}_{F_1}(\mathbf{u}, \mathbf{v}) + (-1)^{v_k} \mathcal{W}_{F_1 \oplus a_{k+1}}(\mathbf{u}, \mathbf{v}),$$

which implies our claim by the induction assumption. □

Theorem 16. *Suppose $f \in \mathcal{G}B_n^8$, with $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2 a_3(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{V}_n$, $a_1, a_2, a_3 \in \mathcal{B}_n$. If f is gbent then $\psi(f)$ is semibent in $\mathcal{B}_{n+2}$.*

Proof. Recall that $\psi(f)(\mathbf{x}, y_1, y_2) = a_1(\mathbf{x})y_1 + a_2(\mathbf{x})y_2 + a_3(\mathbf{x})$. By Lemma 15,

$$\begin{aligned}\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2) =& \mathcal{W}_{a_3}(\mathbf{u}) + (-1)^{v_1} \mathcal{W}_{a_3 \oplus a_1}(\mathbf{u}) \\ &+ (-1)^{v_2} \mathcal{W}_{a_3 \oplus a_2}(\mathbf{u}) + (-1)^{v_1 + v_2} \mathcal{W}_{a_3 \oplus a_2 \oplus a_1}(\mathbf{u}).\end{aligned} \tag{9}$$

Assume first that n is even. Since f is gbent, by [12, Theorem 19], $a_3, a_1 \oplus a_3, a_2 \oplus a_3, a_1 \oplus a_2 \oplus a_3$ are all bent and $\mathcal{W}_{a_3}(\mathbf{u})\mathcal{W}_{a_1 \oplus a_2 \oplus a_3}(\mathbf{u}) = \mathcal{W}_{a_1 \oplus a_3}(\mathbf{u})\mathcal{W}_{a_2 \oplus a_3}(\mathbf{u})$, for all $\mathbf{u} \in \mathbb{V}_n$. Take $\mathcal{W}_{a_3}(\mathbf{u}) = \mu_1(\mathbf{u})2^{n/2}, \mathcal{W}_{a_3 \oplus a_1}(\mathbf{u}) = \mu_2(\mathbf{u})2^{n/2}, \mathcal{W}_{a_3 \oplus a_2}(\mathbf{u}) = \mu_3(\mathbf{u})2^{n/2}, \mathcal{W}_{a_3 \oplus a_2 \oplus a_1}(\mathbf{u}) = \mu_4(\mathbf{u})2^{n/2}$, for some $\mu_i \in \{-1, 1\}, 1 \le i \le 4$. Thus, $\mu_1(\mathbf{u})\mu_4(\mathbf{u}) = \mu_2(\mathbf{u})\mu_3(\mathbf{u})$. Using these in Equation (9), we obtain

$$2^{-n/2}\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2) = \mu_1(\mathbf{u}) + (-1)^{v_1}\mu_2(\mathbf{u}) + (-1)^{v_2}\mu_3(\mathbf{u}) + (-1)^{v_1 \oplus v_2}\mu_4(\mathbf{u}).$$

For $(\mu_1(\mathbf{u}), \mu_2(\mathbf{u}), \mu_3(\mathbf{u}), \mu_4(\mathbf{u}))$ with values in the set

$$\begin{aligned}&(-1,-1,-1,-1), (1,1,-1,-1), (-1,-1,1,1), (-1,1,-1,1),\\ &(1,-1,-1,1), (-1,1,1,-1), (1,-1,1,-1), (1,1,1,1),\end{aligned}$$

$2^{-n/2}\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2)$ takes one of the following values

$$\begin{aligned}&(-1)^{v_1 \oplus v_2 \oplus 1} + (-1)^{v_1 \oplus 1} + (-1)^{v_2 \oplus 1} - 1,\\ &(-1)^{v_1 \oplus v_2} + (-1)^{v_1 \oplus 1} + (-1)^{v_2} - 1,\\ &(-1)^{v_1 \oplus v_2} + (-1)^{v_1} + (-1)^{v_2 \oplus 1} - 1,\\ &(-1)^{v_1 \oplus v_2 \oplus 1} + (-1)^{v_1} + (-1)^{v_2} - 1,\\ &(-1)^{v_1 \oplus v_2} + (-1)^{v_1 \oplus 1} + (-1)^{v_2 \oplus 1} + 1,\\ &(-1)^{v_1 \oplus v_2 \oplus 1} + (-1)^{v_1 \oplus 1} + (-1)^{v_2} + 1,\\ &(-1)^{v_1 \oplus v_2 \oplus 1} + (-1)^{v_1} + (-1)^{v_2 \oplus 1} + 1,\\ &(-1)^{v_1 \oplus v_2} + (-1)^{v_1} + (-1)^{v_2} + 1.\end{aligned}$$

Therefore, $\mathcal{W}_{\psi(f)}$ attains the values $0, \pm 2^{(n+4)/2}$, thus $\psi(f)$ is semibent.

We now consider the case of odd n. Then, by [12, Theorem 19], $a_3, a_1 \oplus a_3, a_2 \oplus a_3, a_1 \oplus a_2 \oplus a_3$ are all semibent and, $\mathcal{W}_{a_3}(\mathbf{u}) = \mathcal{W}_{a_1 \oplus a_3}(\mathbf{u}) = 0$ and $|\mathcal{W}_{a_1 \oplus a_2 \oplus a_3}(\mathbf{u})| = |\mathcal{W}_{a_2 \oplus a_3}(\mathbf{u})| = 2^{(n+1)/2}$, or $|\mathcal{W}_{a_3}(\mathbf{u})| = |\mathcal{W}_{a_1 \oplus a_3}(\mathbf{u})| = 2^{(n+1)/2}$ and $\mathcal{W}_{a_1 \oplus a_2 \oplus a_3}(\mathbf{u}) = \mathcal{W}_{a_2 \oplus a_3}(\mathbf{u}) = 0$.
Case 1. Let $\mathcal{W}_{a_3}(\mathbf{u}) = \mathcal{W}_{a_1 \oplus a_3}(\mathbf{u}) = 0$, $\mathcal{W}_{a_1 \oplus a_2 \oplus a_3}(\mathbf{u}) = \epsilon_1(\mathbf{u}) 2^{(n+1)/2}$, $\mathcal{W}_{a_2 \oplus a_3}(\mathbf{u}) = \epsilon_2(\mathbf{u}) 2^{(n+1)/2}$, with ϵ_1, ϵ_2 taking values from $\{-1, 1\}$. Then from (9) we obtain

$$\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2) = (-1)^{v_2} 2^{(n+1)/2} \left(\epsilon_1(\mathbf{u}) + (-1)^{v_1} \epsilon_2(\mathbf{u})\right),$$

from which we infer that $\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2) \in \{0, \pm 2^{(n+3)/2}\}$, for all combinations of $\epsilon_i(\mathbf{u})$ and v_i, $i = 1, 2$. Therefore $\psi(f)$ is semibent.
Case 2. Let $\mathcal{W}_{a_3}(\mathbf{u}) = \epsilon_1(\mathbf{u}) 2^{(n+1)/2}$, $\mathcal{W}_{a_1 \oplus a_3}(\mathbf{u}) = \epsilon_2(\mathbf{u}) 2^{(n+1)/2}$, $\mathcal{W}_{a_1 \oplus a_2 \oplus a_3}(\mathbf{u}) = \mathcal{W}_{a_2 \oplus a_3}(\mathbf{u}) = 0$, with ϵ_1, ϵ_2 taking values from $\{-1, 1\}$. As before, from (9) we obtain

$$\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2) = 2^{(n+1)/2} \left(\epsilon_1(\mathbf{u}) + (-1)^{v_1} \epsilon_2(\mathbf{u})\right),$$

from which we infer that $\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2) \in \{0, \pm 2^{(n+3)/2}\}$ and therefore $\psi(f)$ is semibent. □

One could ask whether the converse of the previous theorem holds. In general, if we make no other assumptions on the semibent $\psi(f)$, a simple computation reveals that the possible values for $2^{-n}|\mathcal{H}_f(\mathbf{u})|^2$ (if n is even), respectively, $2^{-(n-1)}|\mathcal{H}_f(\mathbf{u})|^2$ (if n is odd) are $4 \pm 2\sqrt{2}, 3 \pm 2\sqrt{2}, 2 \pm \sqrt{2}, 3, 2, 1, 0$ ($\mathcal{H}_f(\mathbf{u})$ in both cases belongs to an 81 element set whose normalized square norms belong to the previous set of values).

Also we would like to recall at this position that by Theorem 19 in [12], $f(\mathbf{x}) = a_1(\mathbf{x}) = 2a_2(\mathbf{x}) + 2^2 a_3(\mathbf{x})$ is gbent if and only if $2^{-\frac{n}{2}} (\mathcal{W}_{a_3}(\mathbf{u}), \mathcal{W}_{a_3 \oplus a_1}(\mathbf{u}), \mathcal{W}_{a_3 \oplus a_2}(\mathbf{u}), \mathcal{W}_{a_3 \oplus a_2 \oplus a_1}(\mathbf{u}))$ is one of the following tuples $(-1,-1,-1,-1)$, $(-1,1,-1,1)$, $(-1,-1,1,1)$, $(-1,1,1,-1)$, $(1,-1,-1,1)$, $(1,1,-1,-1)$, $(1,-1,1,-1)$, $(1,1,1,1)$ if n is even, and $2^{-\frac{n+1}{2}} (\mathcal{W}_{a_3}(\mathbf{u}), \mathcal{W}_{a_3 \oplus a_1}(\mathbf{u}), \mathcal{W}_{a_3 \oplus a_2}(\mathbf{u}), \mathcal{W}_{a_3 \oplus a_2 \oplus a_1}(\mathbf{u}))$ is one of the following tuples $(-1,-1,0,0)$, $(0,0,-1,-1)$, $(-1,1,0,0)$, $(0,0,-1,1)$, $(0,0,1,-1)$, $(1,-1,0,0)$, $(0,0,1,1)$, $(1,1,0,0)$ if n is odd.

In general, for a semibent function $F : \mathbb{V}_{n+2} \to \mathbb{F}_2$ of the form $F(\mathbf{x}, y_1, y_2) = a_3(\mathbf{x}) \oplus y_1 a_1(\mathbf{x}) \oplus y_2 a_2(\mathbf{x})$, the Boolean functions a_1, a_2, a_3 may not satisfy those conditions. In fact, as the following example shows, a generalized Boolean function f which is not gbent, may have a semibent Gray image. Let $n = 3, k = 3$, and $f(x_1, x_2, x_3) = x_1 + 2x_2 + 4x_3$, that is, $a_1(x_1, x_2, x_3) = x_1$,

$a_2(x_1, x_2, x_3) = x_2$, $a_3(x_1, x_2, x_3) = x_3$, and so, $\psi(f)(x_1, x_2, x_3, y_1, y_2) = x_1y_1 \oplus x_2y_2 \oplus x_3$. Then the Walsh-Hadamard spectrum of $\psi(f)$ is $\{0, \pm 8\}$, and so, it is semibent, but of course, f is not gbent (since it would require $a_3, a_1 \oplus a_3, a_2 \oplus a_3, a_1 \oplus a_2 \oplus a_3$ to at least be semibent, which, certainly, they are not).

Below we present the corresponding result on the Gray image of a gbent function in $\mathcal{GB}_n^{16}$.

Theorem 17. *If $f = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2a_3(\mathbf{x}) + 2^3a_4(\mathbf{x}) \in \mathcal{GB}_n^{16}$ is gbent, then its Gray image $\psi(f)$ is semibent in $\mathcal{B}_{n+3}$ if n is odd, and 3-plateaued in $\mathcal{B}_{n+3}$ if n is even.*

Proof. Recall that the Gray image of f is $\psi(f)(\mathbf{x}, y_1, y_2, y_3) = y_1a_1(\mathbf{x}) \oplus y_2a_2(\mathbf{x}) \oplus y_3a_3(\mathbf{x}) \oplus a_4(\mathbf{x})$. By Lemma 15, its Walsh-Hadamard transform is given by

$$\begin{aligned}\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2, v_3) &= \mathcal{W}_{a_4}(\mathbf{u}) + (-1)^{v_1}\mathcal{W}_{a_4\oplus a_1}(\mathbf{u}) \\ &+ (-1)^{v_2}\mathcal{W}_{a_4\oplus a_2}(\mathbf{u}) + (-1)^{v_3}\mathcal{W}_{a_4\oplus a_3}(\mathbf{u}) \\ &+ (-1)^{v_1\oplus v_2}\mathcal{W}_{a_4\oplus a_2\oplus a_1}(\mathbf{u}) + (-1)^{v_1\oplus v_3}\mathcal{W}_{a_4\oplus a_3\oplus a_1}(\mathbf{u}) \\ &+ (-1)^{v_2\oplus v_3}\mathcal{W}_{a_4\oplus a_3\oplus a_2}(\mathbf{u}) + (-1)^{v_1\oplus v_2\oplus v_3}\mathcal{W}_{a_4\oplus a_3\oplus a_2\oplus a_1}(\mathbf{u}).\end{aligned}$$

By going through the 32 cases of Theorem 9 for the Walsh-Hadamard transforms in the expression above (16 for n even and 16 for n odd), we obtain that the Walsh-Hadamard spectrum is $\{0, \pm 2^{3+n/2}\}$ (for n even) and $\{0, \pm 2^{2+(n+1)/2}\}$ (for n odd), hence the claim. □

As we also observed for the $k = 3$ case, the converse of the above theorem is not true, in general. For example, for $n = 4, k = 4$, let $f(x_1, x_2, x_3, x_4) = x_1 + 2x_2 + 4 \cdot 1 + 8(x_3 \oplus x_4)$, and so, $a_1(x_1, x_2, x_3, x_4) = x_1$, $a_2(x_1, x_2, x_3, x_4) = x_2$, $a_3(x_1, x_2, x_3, x_4) = 1$, $a_4(x_1, x_2, x_3, x_4) = x_3 \oplus x_4$. One can see that f is not gbent since the conditions of Theorem 9 are not satisfied, however, the Gray image $\psi(f)$ has Walsh-Hadamard spectrum $\{0, \pm 32\}$ and so it is 3-plateaued in $\mathcal{B}_7$.

Finally we observe that for $k = 2, 3, 4$ the Gray image of a gbent function in $\mathcal{GB}_n^{2^k}$ is $(k-2)$-plateaued when n is odd, and $(k-3)$-plateaued when n is even, which points to a more general theorem.

At last we want to mention that it may be worthwhile to investigate the properties of bent, semibent and plateaued functions which appear as Gray image of a gbent function.

5 Gbent functions and bent functions

In this section we present connections between gbent functions and their components for the general case of gbent functions in $\mathcal{GB}_n^{2^k}$, $k > 1$. In [10] it was shown that a function $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) \in \mathcal{GB}_n^4$, n even, is gbent if and only if a_2 and $a_1 \oplus a_2$ are bent. By Theorem 19 in [12], for a gbent function $f \in \mathcal{GB}_n^8$, n even, given as $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 4a_3(\mathbf{x})$, all Boolean functions, a_3, $a_1 \oplus a_3$, $a_2 \oplus a_3$ and $a_1 \oplus a_2 \oplus a_3$ are bent. For gbent functions in $\mathcal{GB}_n^{16}$, the analog statement follows from our Theorem 9. The general case is dealt with in the following theorem.

Theorem 18. *Let n be even, and let $f(\mathbf{x})$ be a gbent function in $\mathcal{GB}_n^{2^k}$, $k > 1$, (uniquely) given as*

$$f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + \cdots + 2^{k-2}a_{k-1}(\mathbf{x}) + 2^{k-1}a_k(\mathbf{x}),$$

$a_i \in \mathcal{B}_n$, $1 \le i \le k$. Then all Boolean functions of the form

$$g_{\mathbf{c}}(\mathbf{x}) = c_1a_1(\mathbf{x}) \oplus c_2a_2(\mathbf{x}) \oplus \cdots \oplus c_{k-1}a_{k-1}(\mathbf{x}) \oplus a_k(\mathbf{x}),$$

$\mathbf{c} = (c_1, c_2, \ldots, c_{k-1}) \in \mathbb{F}_2^{n-1}$, are bent functions.

Proof. As in Proposition 3, for the gbent function f we denote by $f_{\mathbf{u}}$ the function $f_{\mathbf{u}}(\mathbf{x}) = a_1(\mathbf{x}) + \cdots + 2^{k-2}a_{k-1}(\mathbf{x}) + 2^{k-1}(a_k(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x})$ in $\mathcal{GB}_n^{2^k}$. Again, the integer $b_r^{(\mathbf{u})}$, $0 \le r \le 2^k - 1$, is defined as $b_r^{(\mathbf{u})} = |\{\mathbf{x} \in \mathbb{V}_n : f_{\mathbf{u}}(\mathbf{x}) = r\}|$. By Proposition 3, $b_{r+2^{k-1}}^{(\mathbf{u})} = b_r^{(\mathbf{u})}$ for all $0 \le r \le 2^{k-1} - 1$, except for one element $\rho_{\mathbf{u}} \in \{0, \ldots, 2^{k-1} - 1\}$ depending on $\mathbf{u}$, for which $b_{\rho_{\mathbf{u}}+2^{k-1}}^{(\mathbf{u})} = b_{\rho_{\mathbf{u}}}^{(\mathbf{u})} \pm 2^{n/2}$.

Since it is somewhat easier to follow, we first show the bentness of $a_k(\mathbf{x}) = g_{\mathbf{0}}(\mathbf{x})$. In the second step we show the general case. For $r \neq \rho_{\mathbf{u}}$, $0 \le r \le 2^{k-1}-1$, consider all $\mathbf{x} \in \mathbb{V}_n$ for which $a_1(\mathbf{x})+\cdots+2^{k-2}a_{k-1}(\mathbf{x}) = r$. Since $b_{r+2^{k-1}}^{(\mathbf{u})} = b_r^{(\mathbf{u})}$, for exactly half of these $\mathbf{x}$ we have $a_k(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x} = 0$ (note that the number of these $\mathbf{x}$ must be even). Among all $\mathbf{x} \in \mathbb{V}_n$ for which $a_1(\mathbf{x}) + \cdots + 2^{k-2}a_{k-1}(\mathbf{x}) = \rho_{\mathbf{u}}$, there are $b_{\rho_u}^{(\mathbf{u})}$ for which $a_k(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x} = 0$, and there are $b_{\rho_{\mathbf{u}}+2^{k-1}}^{(\mathbf{u})} = b_{\rho_u}^{(\mathbf{u})} \pm 2^{n/2}$ for which $a_k(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x} = 1$. Hence for the Walsh-Hadamard transform of a_k we get

$$\mathcal{W}_{a_k}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{a_k(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} = \pm 2^{n/2},$$

which shows that a_k is bent.

To show that $g_{\mathbf{c}}$ is bent for every $\mathbf{c} \in \mathbb{F}_2^{k-1}$, we write $f_{\mathbf{u}}(\mathbf{x})$, $\mathbf{u} \in \mathbb{V}_n$, as

$$f_{\mathbf{u}}(\mathbf{x}) = c_1 a_1(\mathbf{x}) + \cdots + c_{k-1} 2^{k-2} a_{k-1}(\mathbf{x}) \ + \ \bar{c}_1 a_1(\mathbf{x}) + \cdots + \bar{c}_{k-1} 2^{k-2} a_{k-1}(\mathbf{x}) + 2^{k-1}(a_k(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}) := h(\mathbf{x}) + \bar{h}(\mathbf{x}) + 2^{k-1}(a_k(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}),$$

where $\bar{c} = c \oplus 1$. Note that every $0 \leq r \leq 2^{k-1} - 1$ in the value set of $a_1(x) + \cdots + 2^{k-2} a_{k-2}(\mathbf{x})$ has then a unique representation as $h(\mathbf{x}) + \bar{h}(\mathbf{x})$. Consider $\mathbf{x}$ for which $h(\mathbf{x}) + \bar{h}(\mathbf{x}) = r + s \neq \rho_{\mathbf{u}}$. Again from $b^{(\mathbf{u})}_{r+2^{k-1}} = b^{(\mathbf{u})}_r$ we infer that for half of those $\mathbf{x}$ we have $a_k(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x} = 0$. As a consequence, we also have

$$g_{\mathbf{c}}(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x} = c_1 a_1(\mathbf{x}) \oplus \cdots \oplus c_{k-1} a_{k-1}(\mathbf{x}) \oplus a_k(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x} = 0$$

for exactly half of those $\mathbf{x}$. (Observe that $h(\mathbf{x}_1) = h(\mathbf{x}_2) = r$ implies $c_1 a_1(\mathbf{x}_1) \oplus \cdots \oplus c_{k-1} a_{k-1}(\mathbf{x}_1) = c_1 a_1(\mathbf{x}_2) \oplus \cdots \oplus c_{k-1} a_{k-1}(\mathbf{x}_2)$.) Similarly as above, among all $\mathbf{x} \in \mathbb{V}_n$ for which $h(\mathbf{x}) + \bar{h}(\mathbf{x}) = \rho_{\mathbf{u}}$, there are $b^{(\mathbf{u})}_{\rho_u}$ for which $a_k(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x} = 0$, and there are $b^{(\mathbf{u})}_{\rho_{\mathbf{u}}+2^{k-1}} = b^{(\mathbf{u})}_{\rho_u} \pm 2^{n/2}$ for which $a_k(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x} = 1$. From this we conclude that $|\{\mathbf{x} \in \mathbb{V}_n \ : \ h(\mathbf{x}) + \bar{h}(\mathbf{x}) = \rho_u \text{ and } f_{\mathbf{u}}(\mathbf{x}) = 1\}| - |\{\mathbf{x} \in \mathbb{V}_n \ : \ h(\mathbf{x}) + \bar{h}(\mathbf{x}) = \rho_u \text{ and } f_{\mathbf{u}}(\mathbf{x}) = 0\}| = \pm 2^{n/2}$. Therefore

$$\mathcal{W}_{g_{\mathbf{c}}}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{g_{\mathbf{c}}(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}} = \pm 2^{n/2},$$

and $g_{\mathbf{c}}$ is bent. □

Theorem 18, which assigns to a gbent function a family of bent functions, provides a necessary condition for a function $f \in \mathcal{GB}_n^{2^k}$ to be gbent. For $k > 2$ the condition is not necessary. As the following example shows, the additional conditions on the Walsh spectra for $k = 3$ given in [12, Theorem 19] and for $k = 4$ given in our Theorem 9, are required (and not implied implicitly by the bentness of the associated Boolean functions). We remark that, as also our Theorem 9 indicates, these additional conditions become complicated as k increases.

Example 19. *Let n be even, a_4 be a bent function, a_1 be an arbitrary Boolean function, both in $\mathcal{B}_n$, set $a_2 := \bar{a}_1, a_3 := 0$. Certainly, for every triple (c_1, c_2, c_3), the function $c_1 a_1(\mathbf{x}) \oplus c_2 a_2(\mathbf{x}) \oplus c_3 a_3(\mathbf{x}) \oplus a_4(\mathbf{x}) = (c_1 \oplus c_2) \oplus a_4(\mathbf{x})$ is bent, but the conditions of Theorem 9 are not satisfied and so, $a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2 a_3(\mathbf{x}) + 2^3 a_4(\mathbf{x})$ is not gbent.*

We close this section with a result which also reveals an inductive approach to the study of gbent functions in $\mathcal{GB}_n^{2^k}$.

Theorem 20. *Let $f \in \mathcal{GB}_n^{2^k}$ with $f(\mathbf{x}) = g(\mathbf{x}) + 2h(\mathbf{x}), g \in \mathcal{B}_n, h \in \mathcal{GB}_n^{2^{k-1}}$. If n is even, then the following statements are equivalent.*

(i) f is gbent in $\mathcal{GB}_n^{2^k}$;

(ii) h and $h+2^{k-2}g$ are both gbent in $\mathcal{GB}_n^{2^{k-1}}$ with $\Im\left(\overline{\mathcal{H}_h^{(2^{k-1})}(\mathbf{u})}\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})\right) = 0$, for all $\mathbf{u} \in \mathbb{V}_n$.

If n is odd, then (ii) implies (i).

Proof. We first show that for n even, h and $h+2^{k-2}g$ are gbent in $\mathcal{GB}_n^{2^{k-1}}$ if f is gbent in $\mathcal{GB}_n^{2^k}$. In a second step, we show that if h and $h+2^{k-2}g$ are both gbent in $\mathcal{GB}_n^{2^{k-1}}$, then f is gbent in $\mathcal{GB}_n^{2^k}$ if and only if $\Im\left(\overline{\mathcal{H}_h^{(2^{k-1})}(\mathbf{u})}\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})\right) = 0$, for all $\mathbf{u} \in \mathbb{V}_n$. This will conclude the proof for both, n even and n odd.

Let $\mathbf{u} \in \mathbb{V}_n$, and for $e \in \{0,1\}$ and $r \in \{0,\ldots,2^{k-1}-1\}$, let

$$S^{(\mathbf{u})}(e,r) = \{\mathbf{x} \in \mathbb{V}_n \ : \ g(\mathbf{x}) = e \text{ and } h(\mathbf{x}) + 2^{k-2}(\mathbf{u}\cdot\mathbf{x}) = r\}.$$

With the notations of Proposition 3, we have $f_{\mathbf{u}}(\mathbf{x}) = f(\mathbf{x}) + 2^{k-1}(\mathbf{u}\cdot\mathbf{x}) = g(\mathbf{x}) + 2(h(\mathbf{x}) + 2^{k-2}(\mathbf{u}\cdot\mathbf{x}))$, and $|S^{(\mathbf{u})}(e,r)| = b_{e+2r}^{(\mathbf{u})}$. If f is gbent, by Proposition 3, there exist $\epsilon \in \{0,1\}$ and $0 \le \rho_{\mathbf{u}} \le 2^{k-2}-1$, for which $|S^{(\mathbf{u})}(\epsilon, \rho_{\mathbf{u}} + 2^{k-2})| = |S^{(\mathbf{u})}(\epsilon,\rho_{\mathbf{u}})| \pm 2^{n/2}$. For $(e,r) \neq (\epsilon,\rho_{\mathbf{u}})$, we have $|S^{(\mathbf{u})}(e, r+2^{k-2})| = |S^{(\mathbf{u})}(e,r)|$. Observing that $\{\mathbf{x} \in \mathbb{V}_n \ : \ h(\mathbf{x}) + 2^{k-2}(\mathbf{u}\cdot\mathbf{x}) = r\} = S^{(u)}(0,r) \cup S^{(u)}(1,r)$, we obtain

$$\mathcal{H}_h^{(2^{k-1})}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{V}_n} \zeta_{2^{k-1}}^{h(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} = \sum_{\mathbf{x}\in\mathbb{V}_n} \zeta_{2^{k-1}}^{h(\mathbf{x})+2^{k-2}(\mathbf{u}\cdot\mathbf{x})} = \pm\zeta_{2^{k-1}}^{\rho_{\mathbf{u}}} 2^{n/2}.$$

Consequently, h is gbent in $\mathcal{GB}_n^{2^{k-1}}$. For $h + 2^{k-2}g \in \mathcal{GB}_n^{2^{k-1}}$ we have

$$\begin{aligned}\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{V}_n} \zeta_{2^{k-1}}^{h(\mathbf{x})+2^{k-2}(\mathbf{u}\cdot\mathbf{x})+2^{k-2}g\mathbf{x}} = \sum_{\substack{e\in\mathbb{F}_2 \\ r\in\mathbb{Z}_{2^{k-1}}}} \sum_{x\in S^{(u)}(e,r)} \zeta_{2^{k-1}}^{r+2^{k-2}e} \\ &= \sum_{\substack{e\in\mathbb{F}_2 \\ r\in\mathbb{Z}_{2^{k-1}}}} |S^{(u)}(e,r)|\zeta_{2^{k-1}}^{r+2^{k-2}e} = \pm\zeta_{2^{k-1}}^{\rho_{\mathbf{u}}+2^{k-2}\epsilon} 2^{n/2},\end{aligned}$$

which implies that also $h + 2^{k-2}g$ is gbent in $\mathcal{GB}_n^{2^{k-1}}$.

To show the condition on $\Im\left(\overline{\mathcal{H}_h^{(2^{k-1})}(\mathbf{u})}\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})\right)$, we write $\zeta_{2^k} = x + yi$,

$\mathcal{H}_h^{(2^{k-1})}(\mathbf{u}) = a+bi$ and $\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u}) = c+di$. From Equation (1), taking the complex norm, squaring and rearranging terms (recall that $|\zeta_{2^k}|^2 = x^2+y^2 = 1$), we get

$$\begin{aligned}2|\mathcal{H}_f^{(2^k)}(\mathbf{u})|^2 &= \frac{1}{2}(a^2+b^2)(1+2x+x^2+y^2) + \frac{1}{2}(c^2+d^2)(1-2x+x^2+y^2)\\ &\qquad - (ac+bd)(\mathbf{x}^2+y^2-1) + 2(ad-bc)y\\ &= |\mathcal{H}_h^{(2^{k-1})}(\mathbf{u})|^2(1+x) + |\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})|^2(1-x)\\ &\quad + 2y\,\Im\left(\overline{\mathcal{H}_h^{(2^{k-1})}(\mathbf{u})}\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})\right).\end{aligned}$$

If h, $h+2^{k-2}g$ are gbent, i.e. $|\mathcal{H}_h^{(2^{k-1})}(\mathbf{u})|^2 = |\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})|^2 = 2^n$ for all $\mathbf{u} \in \mathbb{V}_n$, then we immediately see that $|\mathcal{H}_f^{(2^k)}(\mathbf{u})|^2 = 2^n$ for all $\mathbf{u} \in \mathbb{V}_n$, and hence f is gbent if and only if $\Im\left(\overline{\mathcal{H}_h^{(2^{k-1})}(\mathbf{u})}\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})\right) = 0$, for all $\mathbf{u} \in \mathbb{V}_n$. □

Remark 21. *For n even and $k = 2$, Theorem 20 recovers the result in* [10] *on the relation between gbentness and bentness of the components (see also* [12, Corollary 15 & 16]*): The function $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) \in \mathcal{GB}_n^4$ is gbent if and only if both Boolean functions a_2 and $a_1 \oplus a_2$ are bent.*
If n is odd, as an example for the implication $(ii) \Longrightarrow (i)$ we can take $g = 0$, and an arbitrary h gbent in $\mathcal{GB}_n^{2^{k-1}}$. Certainly, the conditions from (ii) are readily satisfied.

Remark 22. *In* [4]*, conditions are derived for the gbentness of some functions $f \in \mathcal{GB}_n^q$ of the form $f(\mathbf{x}) = \frac{q}{2}a(x) + rb(x)$, $r \in [q/4, 3q/4]$, a, b in $\mathcal{GB}_n^q$ or $\mathcal{B}_n$.*

Analyzing the components of gbent functions in $\mathcal{GB}_n^{2^k}$, n even, we obtained some necessary conditions on gbentness (Theorem 18) and necessary and sufficient conditions on gbentness (Theorem 20), where the latter are sufficient but not necessary also for odd n, however not very simple to check. Presumably, one could also attempt to extend our Theorem 9 to the case $k = 5$, although, we doubt that the complicated equations one would obtain can easily be analyzed, and certainly they do not give any further insight into the nature of gbent functions. We believe that the next step in completely characterizing gbentness for all k, should be to find a more "inductive" approach, where one would connect gbentness of f in $\mathcal{GB}_n^{2^k}$ to its components

in $\mathcal{GB}_n^{2^{k-j}}$, $1 \leq j \leq 4$, and using the results in this paper.

Acknowledgements. Work by P.S. started during a very enjoyable visit at RICAM. Both the second and third named author thank the institution for the excellent working conditions. The second author is supported by the Austrian Science Fund (FWF) Project no. M 1767-N26.

References

[1] C. Carlet, *$\mathbb{Z}_{2^k}$-linear Codes*, IEEE Trans. Inf. Theory 44:4 (1998), 1543–1547.

[2] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications, Academic Press, San Diego, CA, 2009.

[3] S. Gangopadhyay, E. Pasalic, P. Stănică, *A note on generalized bent criteria for Boolean functions*, IEEE Trans. Inform. Theory 59:5 (2013), 3233–3236.

[4] S. Hodžić, E. Pasalic, *Generalized bent functions – Some general construction methods and related necessary and sufficient conditions*, Cryptogr. Commun. 7 (2015), 469–483.

[5] P.V. Kumar, R.A. Scholtz, L.R. Welch, *Generalized bent functions and their properties*, J. Combin theory – Ser. A 40 (1985), 90–107.

[6] M.G. Parker, A. Pott, *On Boolean functions which are bent and negabent*, In: Sequences, subsequences, and consequences, LNCS 4893, Springer, Berlin, 2007, 9–23.

[7] J. Rouse, *Explicit bounds for sums of squares*, Math. Res. Lett. 19:2 (2012), 359–376.

[8] K.U. Schmidt, *Quaternary constant-amplitude codes for multicode CDMA*, IEEE Trans. Inform. Theory 55:4 (2009), 1824–1832.

[9] K.U. Schmidt, *$\mathbb{Z}_4$-valued quadratic forms and quaternary sequence families*, IEEE Trans. Inform. Theory 55:12 (2009), 5803–5810.

[10] P. Solé, N. Tokareva, *Connections between Quaternary and Binary Bent Functions*, Prikl. Diskr. Mat. 1 (2009), 16–18 (see also, http://eprint.iacr.org/2009/544.pdf).

[11] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A.K. Gangopadhyay, S. Maitra, *Investigations on bent and negabent functions via the nega-Hadamard transform*, IEEE Trans. Inform. Theory 58:6 (2012), 4064–4072.

[12] P. Stănică, T. Martinsen, S. Gangopadhyay, B.K. Singh, *Bent and generalized bent Boolean functions*, Des. Codes Cryptogr. 69 (2013), 77–94.

[13] W. Su, A. Pott, X. Tang, *Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree*, IEEE Trans. Inform. Theory 59:6 (2013), 3387–3395.

[14] N. Tokareva, *Generalizations of bent functions: a survey of publications*, (Russian) Diskretn. Anal. Issled. Oper. 17 (2010), no. 1, 34–64; translation in J. Appl. Ind. Math. 5:1 (2011), 110–129.